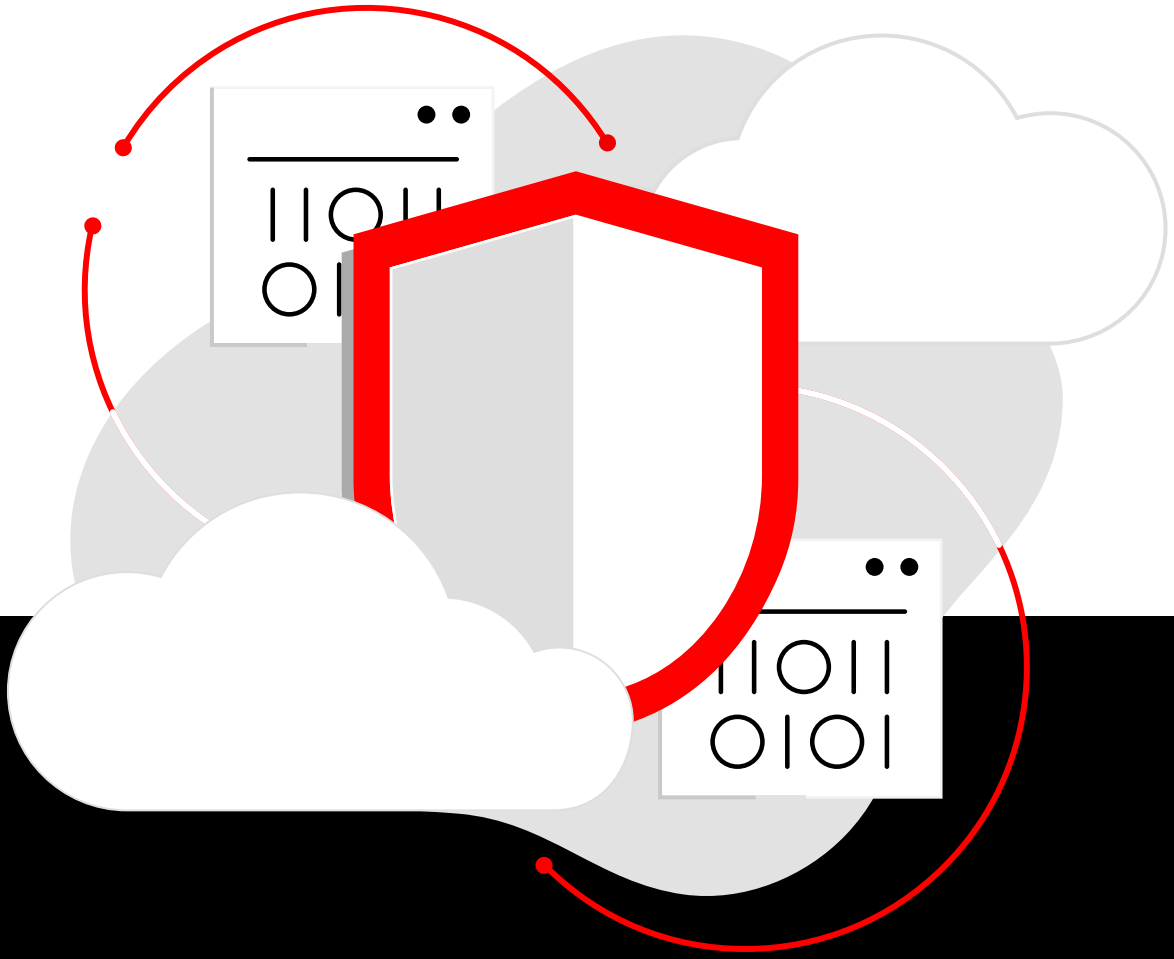
Red Hat



Modernize and secure your application life cycles with DevSecOps

Contents

Introduction

Application security is critical in a digital world

As an increasing number of organizations adopt cloud, container, and microservices technologies to compete in a digital world, security remains a top concern. In fact, 50% of senior IT leaders at enterprises cite cybersecurity as a top-three priority for technology initiatives.[1] At the same time, 86% expect their organization's pace of digital transformation to increase in 2021.[1]

These new technologies require a different approach to security, as traditional, perimeter-based approaches are not effective in distributed environments. Additionally, development speed and deployment flexibility increase with DevOps and cloud-native methodologies, making it important to consider security earlier in the process. Applying security measures only at the end of development cycles often results in delivery delays and lower protection.

Adopting **DevSecOps** approaches and practices can help you better protect your application environment and your business.

What is DevSecOps?

DevSecOps extends the collaborative culture of DevOps to incorporate security throughout your application life cycles. It encompasses people, processes, and technology to make security more pervasive in distributed environments.

Through DevSecOps, security becomes a shared responsibility across teams, rather than a set of tasks owned by one team and applied at the end of the development and deployment process. Security, development, and operations teams work together, sharing information, feedback, lessons learned, and insights. This approach allows security to be integrated from the start of application development and infrastructure deployment, increasing protection and reducing risks.

Benefits of DevSecOps

Improve security and reduce risk.

Address security issues in development – rather than in production – to better safeguard your applications and reduce the number of deployments that are delayed or stopped due to failed policy checks.

Fix security issues faster.

Apply modern security practices and tools that encourage collaboration and incorporate automation to accelerate release cycles, reduce the time needed to fix security issues in production, and save time and money.

Increase compliance and visibility.

Adopt automated processes and tools that reduce the risk of manual errors and increase predictability and repeatability to improve compliance and simplify audit processes.

1 *Flexera. "2021 Flexera State of Tech Spend Report," January 2021.*

DevSecOps implementation challenges

While DevSecOps approaches deliver many benefits, several factors can make implementing DevSecOps difficult.

- **Evolving security landscape.** Security threats and regulations—including business, technical, and geographical requirements—continue to change at a rapid pace, making it difficult to stay up to date.
- **Application environment complexity.** It can be challenging to understand the connections and security implications of all of the different technologies—like containers, microservices, and cloud services—that make up complicated, large-scale application environments.
- **Inefficient existing tools and processes.** Many teams begin by applying their existing tools and processes to DevSecOps initiatives, but find that this approach does not support their goals over time.
- **Multiple security tools.** Choosing, testing, integrating, and maintaining the right selection of security tools for your organization takes time, research, and ongoing effort.

Successful DevSecOps relies upon culture, process, and technology

Securing application life cycles with DevSecOps requires change and alignment in three areas: culture, process, and technology.

Culture

Promote collaboration and shared goals amongst your development, operations, and security teams. Help each team understand the reasons and methods for building security into your application life cycles.

Process

Standardize, document, and automate your processes and workflows to improve efficiency and security throughout your application life cycles.

Technology

Integrate your application development, deployment, and operations platforms, tools, and processes into a single, cohesive system.

Learn more about the basics of DevSecOps

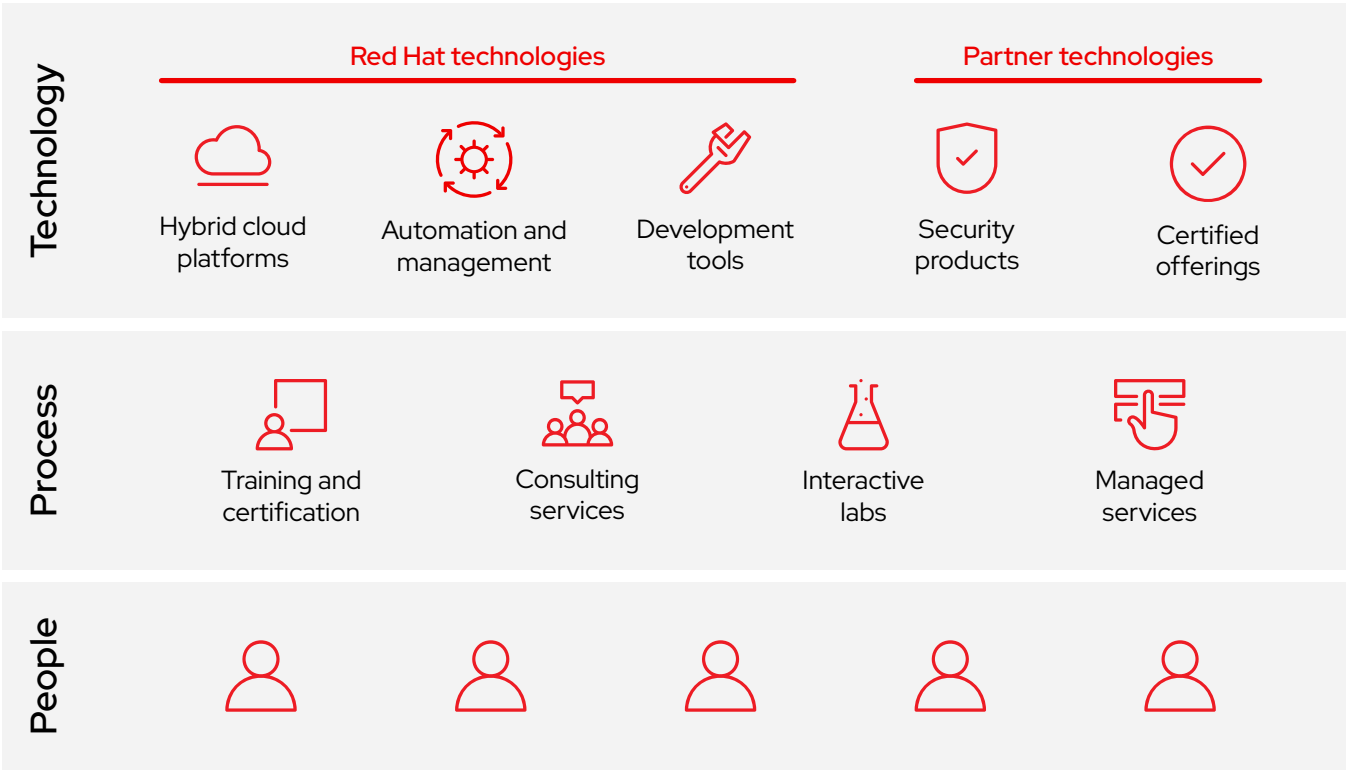
Read the **Why your DevSecOps practice may be falling short blog post** to learn more about the changes needed to successfully implement DevSecOps. Read the **Boost hybrid cloud security e-book** to learn how to protect your business with cloud-native security approaches.

Red Hat DevSecOps strategy

Red Hat brings together a certified partner ecosystem, extensive expertise, and innovative platforms for building, securing, and deploying applications across hybrid cloud environments. This combination allows you to implement comprehensive DevSecOps solutions to improve application security, reduce risks, increase performance, and maximize the value of your investments.

With a trusted content supply chain, support from a dedicated security team, and key security feature backports, Red Hat® platforms provide an ideal foundation for DevSecOps solutions. Our partners extend and enhance this foundation with innovative, integrated products for applying security and automation across application life cycles. Finally, we offer **training and certification courses**, **interactive labs**, **consulting engagements**, and **managed offerings** to help you successfully implement DevSecOps.

Together, we meet you wherever you are in your DevSecOps journey. With our modular, expandable solutions and expert services, you can deploy what you need today, adapt to future change, and learn the methods and approaches needed for efficient, effective DevSecOps adoption.



Build an open DevSecOps foundation with Red Hat products

Red Hat OpenShift

Red Hat OpenShift® is an enterprise-ready, security-focused hybrid cloud platform that includes built-in DevOps tools and security capabilities that are enabled by default. This platform works with partner and third-party security tools and technologies to enhance security and implement strong DevSecOps. Read the Red Hat OpenShift security guide to learn how security is addressed throughout the technology stack.

Try it for free

Key security features

- Security-Enhanced Linux (SELinux)
- Security context constraints (SCC)
- Identity and access management
- Data encryption
- Federal Information Processing Standards (FIPS) mode

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform is a flexible, powerful platform that can automate and integrate security solutions and provides a common language between your security tools. Learn about automation use cases.

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux® CoreOS is a lightweight, immutable, container-optimized operating system based on the security-focused foundation of Red Hat Enterprise Linux and used within Red Hat OpenShift.

Red Hat Quay

Red Hat Quay is a distributed and highly available container image registry that lets you build, distribute, and deploy containers.

Red Hat CodeReady Workspaces

Red Hat CodeReady Workspaces is a tool that lets developers code, build, and test in containers running on Red Hat OpenShift.

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes provides a cloud-native architecture for container security that protects applications from build to runtime.

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes controls clusters and applications from a single console, with built-in security policies.

Gain flexibility and reliability with a certified security partner ecosystem

No single vendor offers all the capabilities needed to fully implement effective DevSecOps. Additionally, each organization is different and requires a unique combination of products and technologies to meet their needs.

Red Hat collaborates with **innovative, industry-leading security partners** to deliver complete solutions based on certified integrations, container images, and **Red Hat OpenShift operators**. You can confidently choose the partners, products, and technologies that best fit your needs at all times, knowing they will work reliably and consistently together. These solutions are also backed by expert services, support, and training to help you implement DevSecOps culture, processes, and tools successfully.

Red Hat security partner ecosystem benefits

Choice

Choose the products and vendors that best meet your organization's needs at all times.

Certification

Build your solution with confidence knowing that all components are certified to work together reliably.

Expertise

Take advantage of the combined DevSecOps expertise and experience of Red Hat and partners.

Services

Get help implementing DevSecOps culture, processes, and tools within your organization.

Training

Learn best practices and gain the skills you need to adopt DevSecOps approaches.

Red Hat Vulnerability Scanner Certification

Red Hat Vulnerability Scanner Certification minimizes discrepancies between vulnerability scanner results. Red Hat works with certified security partners to deliver more accurate and reliable container vulnerability scanning results for Red Hat-published images and packages.

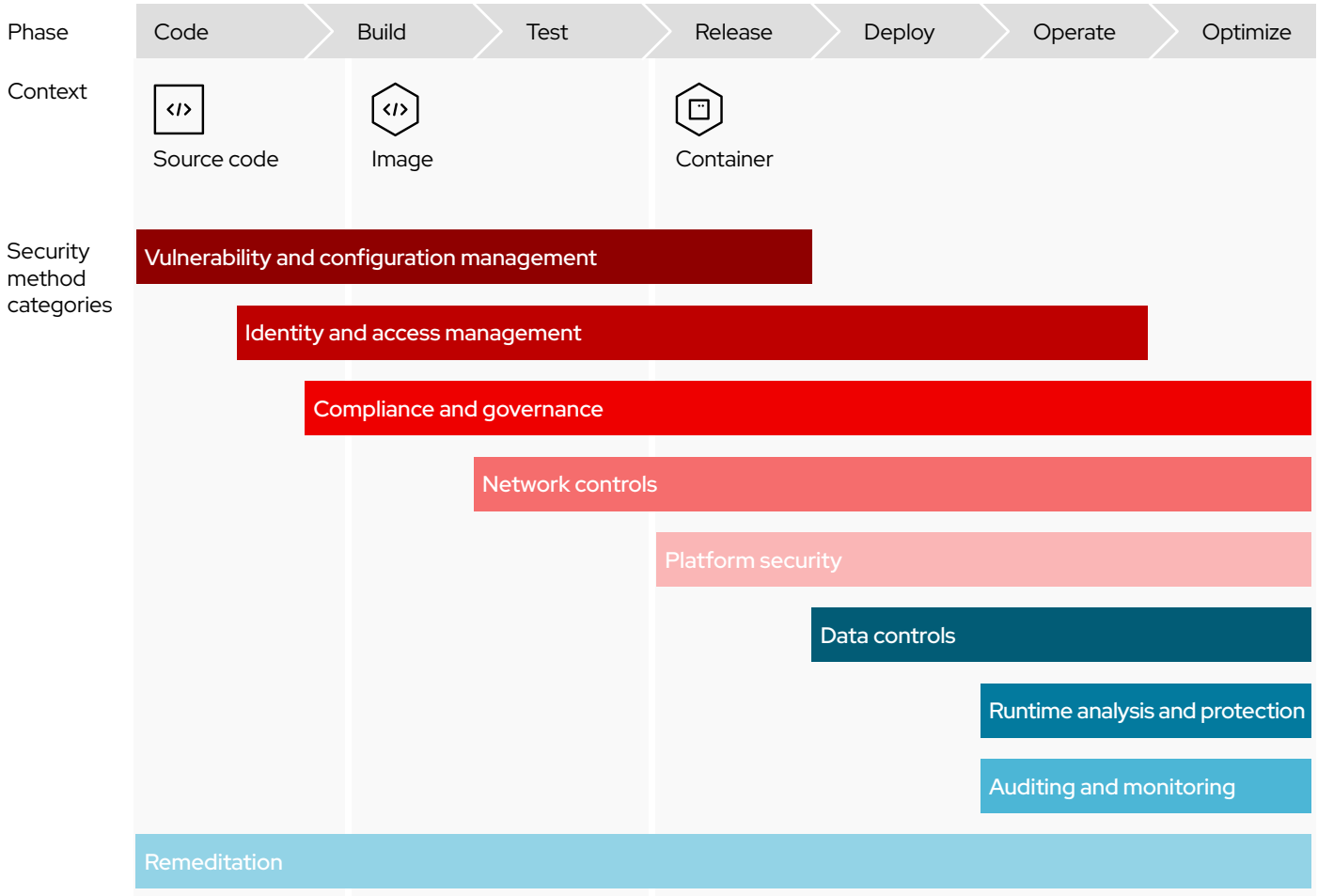
- Minimize false positives and other discrepancies.
- Free up time and budget for strategic projects and initiatives.
- Achieve greater levels of assurance.
- Improve accuracy with centralized data for Red Hat-published images.
- Simplify vulnerability management.

Find certified products

Create complete DevSecOps solutions

Red Hat offers a framework for building highly scalable, comprehensive DevSecOps solutions that address security requirements throughout your application life cycles. Created with our security partners, this framework can help you implement DevSecOps in your organization according to your current and expected needs.

The Red Hat DevSecOps framework maps a comprehensive set of security tool and methods – categorized by function – onto the application development life cycle.



Read the overview

Choose the security methods and products that fit your needs

The Red Hat DevSecOps framework organizes 34 primary security methods into 9 categories. Red Hat and certified partner technologies align with one or more of these methods to help you build a complete DevSecOps solution that meets your organization's needs and adapts to future change.

Vulnerability and configuration management

- Static application security testing (SAST)
- Static code analysis (SCA)
- Interactive application security testing (IAST)
- Dynamic application security testing (DAST)
- Configuration management
- Image risk

Identity and access management

- Authentication
- Authorization
- Secrets vault
- Hardware security modules (HSM)
- Provenance

Compliance and governance

- Regulatory compliance auditing
- Compliance controls and remediation

Network controls

- Container network interface (CNI) plugins
- Network policies
- Traffic control
- Service mesh
- Visualization
- Package analysis
- Application programming interface (API) management

Platform security

- Secure host
- Container platform
- Namespace
- Isolation
- Kubernetes and container hardening

Data controls

- Data protection and encryption

Runtime analysis and protection

- Admission controller
- Application behavior analysis
- Threat defense

Auditing and monitoring

- Cluster monitoring
- Security information and event management (SIEM)
- Forensics

Remediation

- Security orchestration, automation, and response (SOAR) platforms
- Automatic resolution

Find certified partners

Partner highlight

Sysdig

Sysdig helps organizations confidently run workloads in the cloud with security-focused DevOps technologies. Sysdig's products for monitoring and securing applications, workloads, and containers help hundreds of companies ship cloud-native applications faster.

Together, Red Hat and Sysdig help enterprises rapidly adopt cloud-native approaches. Sysdig Secure DevOps Platform, Sysdig Secure, and Sysdig Monitor work with Red Hat OpenShift and Red Hat Advanced Cluster Management for Kubernetes to deliver unified security, compliance, and monitoring for private, hybrid, and multicloud environments. These solutions help you secure build pipelines, detect and respond to threats, continuously validate cloud posture and compliance, and monitor performance. Built on an open source stack, Sysdig's cloud-native monitoring, security, and forensics capabilities give you the insight and control needed to move to the cloud with less risk.

Red Hat and Sysdig solutions help you:

- Scan images directly within your continuous integration/continuous deployment (CI/CD) pipelines.
- Monitor performance and availability at cloud scale.
- Implement continuous compliance and runtime security.
- Validate Red Hat OpenShift infrastructure configurations.
- Troubleshoot and respond to issues more easily.

2020

Red Hat Rising Star Partner of the Year for public sector[2]

Manage security risk.

Identify and fix vulnerabilities throughout your pipelines. Detect and block threats at runtime with automated policies and controls. Respond to and investigate incidents, even after containers have been retired.

Boost performance and availability.

Survey and retain millions of metrics. Monitor health and performance across your environment to proactively find and fix issues. Troubleshoot problems inside clusters, pods, and containers more easily.

Validate cloud compliance.

Validate Red Hat OpenShift environment compliance with common standards. Audit clusters, nodes, and containers via detailed activity reports. Implement file-integrity monitoring across container life cycles.

Access integrations

2 Red Hat blog. "Red Hat awards North American partners for commitment to open source innovation," 23 April 2020.

Partner highlight

Synopsys

Synopsys provides static, software composition, and dynamic analysis solutions for rapidly building secure software. With a combination of industry-leading tools, services, and expertise, Synopsys helps organizations apply DevSecOps to optimize security and quality throughout software development life cycles.

Red Hat and Synopsys help you create high-quality, security-focused code to minimize risks while maximizing speed and productivity. **Synopsys Black Duck software composition analysis (SCA)** integrates with Red Hat OpenShift to increase visibility into, and control over, security vulnerabilities and policy violations in the open source code within your containers. **Black Duck for OpenShift** automatically discovers, scans, monitors, and inspects all container images in your Red Hat OpenShift clusters to identify open source security and compliance risks at any phase of container construction. The software also helps you ensure vulnerable containers are not pushed into production and respond quickly to new vulnerabilities that affect running containers.

The Black Duck for OpenShift solution:

- Provides a complete list of all third-party open source code in each container image and annotates your pods with vulnerability and policy metadata.
- Immediately alerts you of new vulnerabilities that affect your containers and identifies which images and containers are impacted.
- Understands open source forks and backports and marks vulnerabilities as patched when appropriate, reducing the number of vulnerabilities that require investigation.
- **Integrates** with Red Hat Advanced Cluster Management for Kubernetes to ensure consistent deployment across all clusters.

Automatically scan container images.

Continuously monitor open source code.

Identify security vulnerabilities.

"Synopsys and Red Hat share a similar vision for the future of secure application development and deployment and, together, we look forward to helping organizations build trust in their containerized applications."

Vatsal Sonecha
VP of Business Development, Synopsys

Access integrations

Partner highlight

Palo Alto Networks

Palo Alto Networks delivers innovation to support secure digital transformation even as the pace of change accelerates. The company provides a portfolio of security solutions that help more than 60,000 customers worldwide safeguard their businesses.

Red Hat and Palo Alto Networks help you protect your environment with cloud-native security and compliance throughout the entire development life cycle. Prisma Cloud by Palo Alto Networks works with Red Hat OpenShift to deliver comprehensive cloud security posture management (CSPM) and cloud workload protection (CWP) for your deployments. This solution provides complete life-cycle security for hosts, containers, and serverless, as well as visibility into and governance over your security posture.

Red Hat partner since

2017

Key features and benefits

Vulnerability management

Embed security from development to production with vulnerability detection, understanding, and prevention at every stage of the application life cycle.

Compliance

Easily implement and maintain compliance for Center for Internet Security (CIS) benchmarks, external compliance regimes, and custom requirements.

CI/CD security

Integrate security directly into your continuous integration (CI) processes to find and fix problems before they are deployed into production.

Runtime defense

Apply security at scale with machine learning that automatically creates least-privileged, allow-list-based runtime models for all application versions.

Web application and interface security

Protect against layer 7 and Open Web Application Security Project (OWASP) Top Ten threats across your public and private cloud environments.

Access controls

Establish and monitor access controls for workloads and applications while integrating with existing identity, access, and secrets management tools.

Access integrations

Partner highlight

CyberArk

CyberArk applies a unique security-first approach to identity-based privileged access control. The company delivers complete solutions to protect secrets and credentials used by people, applications, scripts, and machines across enterprises, clouds, and DevOps environments.

Together, Red Hat and CyberArk help you improve the security of your container environments and automation scripts. Enterprise-wide privileged access security policies provide visibility, auditing, enforcement, and secrets management to mitigate business risks. CyberArk DevSecOps products – including Conjur Secrets Manager and Credential Providers – integrate with Red Hat OpenShift and Red Hat Ansible Automation Platform to protect, rotate, monitor, and manage privileged credentials for people, applications, scripts, and other non-human identities using a centralized platform. With a single point of control across your organization, you can unify security management, reduce security vulnerabilities, minimize attack surfaces, and streamline operations.

The modular architecture lets you deploy each component independently to customize protection across hybrid cloud, multicloud, containerized, and DevOps environments. Strong runtime authentication and role-based access controls ensure that only authorized pods and containers receive secrets. Integration with Red Hat Ansible Automation Platform allows playbooks to access managed secrets and eliminate the need for manual secret entry and rotation. This integration also lets you automate remediation tasks in response to detected security incidents.

Unify security.

Centrally manage and secure secrets and privileged access credentials across your infrastructure, according to your policies.

Simplify operations.

Allow developers and automation engineers to secure, manage, and rotate the secrets and credentials they use based on your policies.

Improve consistency.

Consistently protect secrets and credentials used by applications, scripts, and people accessing your management consoles.

Watch the webinar

Partner highlight

Tigera

Tigera transforms how companies secure, observe, and troubleshoot Kubernetes networking and microservices communication.

Red Hat and Tigera help organizations build security into their Kubernetes environments by monitoring, analyzing, and managing network traffic. Certified with Red Hat OpenShift, **Tigera Calico Enterprise** helps you successfully operate, optimize, and protect critical containerized applications across cloud environments. The Kubernetes-native architecture embeds the solution into your application environment to provide detailed security controls and improved visibility between the network and microservices layers. This solution also integrates with your existing security tools, environments, and security operations centers (SOCs) to provide additional controls and capabilities for modern workloads. Improve application security across development, test, and production environments with zero-trust networking, egress access controls, traffic visibility, threat protection and defense, and automated compliance audit reports.

Extend your security capabilities.

Protect applications via existing firewalls, least-privileges security, and interpod traffic encryption.

Gain network visibility.

Access network flows to debug connectivity, threat hunt, and automate compliance reporting.

Ensure compliance.

Monitor application compliance and deliver real-time alerts for non-compliant workloads.

Access the operator

Partner highlight

Aqua Security

Aqua Security helps customers innovate and run their businesses with minimal friction. The company provides threat prevention, detection, and response automation throughout application life cycles to improve security across all aspects of your environment.

Red Hat and Aqua Security help you manage and scale your cloud-native workloads more securely across on-site, hybrid, and cloud infrastructure. The Aqua Cloud Native Security Platform integrates with Red Hat OpenShift to provide risk-based vulnerability management, detailed runtime protection, and comprehensive infrastructure assurance and compliance. The solution empowers development, security, and operations teams to deliver applications more securely, protect against threats at runtime, and assess and remediate infrastructure configurations based on policy checks.

Key features and benefits

Support DevSecOps approaches.

- Analyze code, configurations, and permissions for Red Hat OpenShift registry images at scale.
- Prioritize vulnerabilities by risk.
- Automate build processes through integration with CI/CD pipelines.

Protect applications at runtime.

- Detect and automatically mitigate unauthorized container activity without disrupting applications.
- Enforce container immutability by identifying and preventing unauthorized changes from standard images.

Improve software supply chain security.

- Run and validate images in protected preproduction test environments.
- Identify advanced malware that static scanners may not detect before deployment.

Maintain infrastructure compliance.

- Scan and validate hundreds of configuration and control policies for compliance with best practices and Center for Internet Security (CIS) benchmarks.
- Enforce role-based access controls (RBAC) via Open Policy Agent (OPA) based declarative assurance policies.

Access integrations

Ready to start your DevSecOps journey?

Application security is a requirement for digital businesses. Adopting DevSecOps approaches can help you better protect your application environment and your business.

Red Hat combines an innovative technology foundation with a comprehensive DevSecOps ecosystem and extensive expertise to help you successfully implement DevSecOps throughout your organization.

- Choose from a variety of certified, industry-leading tools and technologies to meet your needs now and in the future.
- Learn best practices and gain DevSecOps skills with expert training resources.
- Deploy faster with specialized services and consulting engagements.

Learn more about implementing DevSecOps with Red Hat:
redhat.com/en/partners/devsecops

F29623_0721_KVM

Red Hat